REMARKS

In view of the above amendment and the following discussion, the Applicant submits that none of the claims now pending in the application is unpatentable under the provisions of 35 U.S.C. §103. Thus, the Applicant believes that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-2, 4-6, 8-10, 12-14, and 16 UNDER 35 U.S.C. § 103

The Examiner has rejected claims 1-2, 4-6, 8-10, 12-14, and 16 in the Office Action under 35 U.S.C. §103 as being unpatentable over the Bailey, III reference (U.S. Patent 5,659,614, issued August 19, 1997, hereinafter referred to as "Bailey") in view of Cane et al. (U.S. Patent 5,940,507, issued August 17, 1999, hereinafter referred to as "Cane"). The Applicant respectfully traverses the rejection.

Bailey teaches a method and system for creating and storing a backup copy of file data stored on a computer. "The file data to be backed up is encrypted using multiple, indirect encryption keys, variable block lengths, and variable algorithms based on a client-selected string of characters. The files are thereafter encrypted again at the client site prior to transmission to the backup site. A program registry is maintained at the backup site that contains a master copy of many commercially-available files. The incoming files received from the client site are compared to the files in the program registry. If an incoming file is located in the registry, the file is replaced by a token identifying the commercially-available file and the token is stored at the backup facility" (see Bailey, Abstract).

Cane teaches an information process system that provides archive/backup support with privacy assurance by encrypting relevant stored data. Notably, data generated on a source system is encrypted, the key used thereby is separately encrypted, and both the encrypted data and encrypted key are transmitted to and maintained by a data repository system (see Cane, Abstract)

The Examiner's attention is directed to the fact that the combination of Bailey and Cane fails to teach or suggest the novel concept of generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle, as positively claimed by the Applicant in claims 1 and 9. In addition, the Applicant submits that the

combination of Bailey and Cane fails to teach or suggest the checking for an authentication code in the compressed bundle, as positively claimed by the Applicant in claims 5 and 13. Specifically, Applicant's independent claims 1, 5, 9, and 13 positively recite:

> 1. A method of backing up one or more files on a local device onto remote servers over a network comprising:
> deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
> compressing one or more files and adding each of the files to a bundle;
> generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
> encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added)
>
> 5. A method of restoring one or more files on remote servers to a local device over a network comprising:
> deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
> decrypting a bundle received from the remote server using the second cryptographic key;
> checking an authentication code in the bundle using the first cryptographic key; and
> decompressing one or more files from the bundle. (Emphasis added)
>
> 9. A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:
> deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
> compressing one or more files and adding each of the files to a bundle;
> generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
> encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added)
>
> 13. A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:
> deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
> decrypting a bundle received from the remote server using the second cryptographic key;
> checking an authentication code in the bundle using the first cryptographic key; and
> decompressing one or more files from the bundle. (Emphasis added)

The Applicant's invention provides a method and device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network (see claims 1 and 9). More specifically, the invention prompts for a

user-provided passphrase that is used to derive two cryptographic keys. An authentication code for a bundle (i.e., compressed data) is generated using the first of the two cryptographic keys. The authentication code is then added to the bundle, wherein the entire bundle is subsequently encrypted using the second cryptographic key. Lastly, the encrypted bundle is sent to the remote server to complete the backup process.

Likewise, the Applicant's invention provides a method and device-readable medium storing program instructions for restoring files on remote servers to a local device over a network (see claims 5 and 13). The restoring process is similar to the backup process described above except it is executed in reverse order.

As indicated by the Examiner on page 3 of the Office Action, Bailey fails to disclose the generation of an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle. However, the Examiner alleges that Cane teaches this limitation.

In response, the Applicant respectfully disagrees and submits that Cane teaches a key generator that generates a secondary key and uses this key to encrypt the file to produce an encrypted file. A master key is then obtained and used to encrypt the secondary key and produce an encrypted key that is separate from the encrypted file (see Cane, column 3, lines 56-61). The encrypted file and the encrypted key are then transmitted as separate entities (i.e., not in a single bundle or file) to the archive server as indicated in separate steps 116 and 118 (see Cane, FIG. 2).

Therefore, the Applicant submits that Cane does not bridge the substantial gap existing between the Applicant's invention and Bailey. More specifically, the Applicant contends that Cane does not teach, suggest, or mention a bundle comprising an authentication code and files that have been encrypted together as set forth in claims 1 and 9. The Examiner's attention is directed to the fact that Bailey in view of Cane fails to disclose or suggest the novel concept of generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle as claimed in Applicant's independent claims 1 and 9. Therefore, the Applicant submits that independent claims 1 and 9 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Similarly, Bailey in view of Cane fails to disclose or suggest the novel concept of checking an authentication code that was encrypted in the bundle using a first cryptographic key as claimed in Applicant's independent claims 5 and 13. As indicated on page 4 of the Office Action by the Examiner, Bailey does not expressly disclose the checking of an authentication code in the bundle using the first cryptographic key. However, the Examiner alleges that Cane teaches this limitation. In response, the Applicant submits that Bailey and Cane do not disclose, mention, or suggest the checking of an authentication code in a bundle using the first cryptographic key. More specifically, the Applicant contends that Cane only teaches an archive server that first writes the encrypted file to a medium and subsequently writing the encrypted key to another medium separately. Notably, the Applicant submits that Cane does not teach a checking process of any type. Furthermore, the Applicant contends that since a bundle comprising an authentication code along with a plurality of files is not taught by Cane, it is impossible for the bundle to be checked (i.e., since a bundle does not exist). Since Cane does not teach this aspect, the Applicant submits that Cane does not bridge the substantial gap existing between Bailey and the Applicant's invention. Therefore, the Applicant submits that independent claims 5 and 13 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Furthermore, dependent claims 2, 4, 6, 8, 10, 12, 14, and 16 depend, either directly or indirectly, from claims 1, 5, 9, and 13 and recite additional features therefrom. As such, and for the exact same reason set forth above, the Applicant submits that claims 2, 4, 6, 8, 10, 12, 14, and 16 are not made obvious by Bailey in view of Cane. Therefore, the Applicant submits that dependent claims 2, 4, 6, 8, 10, 12, 14, and 16 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

II. REJECTION OF CLAIMS 3, 7, 11, AND 15 UNDER 35 U.S.C. §103

The Examiner has rejected claims 3, 7, 11, and 15 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Cane in further view of the Walmsley reference (U.S. Publication No. 2004/0049468, published March 11, 2004, hereinafter referred to as "Walmsley"). The Applicant respectfully traverses the

rejection.

Bailey and Cane have been discussed above.

Walmsley teaches "a consumable authentication method for validating the existence of an untrusted chip. A random number is encrypted using a first key and sent to an untrusted chip. In the untrusted chip it is decrypted using a secret key and re-encrypted together with a data message read from the untrusted chip. This is decrypted so that a comparison can be with the generated random number and the read data message" (see Walmsley, Abstract).

The Applicant submits that Walmsley does not bridge the substantial gap existing between the Applicant's invention and the combination of Bailey and Cane. More specifically, the Applicant contends that Walmsley does not teach, suggest, or mention an authentication code or bundle as set forth in claims 1, 5, 9, and 13. The Examiner's attention is directed to the fact that Bailey in view of Cane in further view of Walmsley fails to disclose or suggest the novel concept of generating an authentication code for a bundle that is ultimately added to and encrypted with the bundle as claimed in Applicant's independent claims 1 and 9 from which claims 3 and 11 depend. Similarly, Bailey in view of Cane in further view of Walmsley fails to disclose or suggest the novel concept of checking an authentication code that was encrypted in the bundle using a first cryptographic key as claimed in Applicant's independent claims 5 and 13 from which claims 7 and 15 depend.

Consequently, the Applicant submits that claims 1, 5, 9, and 13 would not be made obvious by the teaching of Bailey in view of Cane in further view of Walmsley, and therefore, are patentable under 35 U.S.C. §103.

Since claims 3, 7, 11, and 15 depend, either directly or indirectly, from claims 1, 5, 9, and 13, and recite additional features thereof, the Applicant submits that 3, 7, 11, and 15 are also not made obvious by the teaching of Bailey in view of Cane in further view of Walmsley. Therefore, the Applicant submits that claims 3, 7, 11, and 15 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Conclusion

Thus, the Applicant submits that all of the claims now fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicant believes that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

8/4/05

Moser, Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404